

ENDOMORPHISM ALGEBRAS OF QM ABELIAN SURFACES

CHIA-FU YU

ABSTRACT. We determine endomorphism algebras of abelian surfaces with quaternion multiplication.

1. INTRODUCTION

In this paper, we determine all possible endomorphism algebras of abelian surfaces with quaternion multiplication (QM). Let D be an indefinite quaternion division algebra over the field \mathbb{Q} of rational numbers. We would like to find out all \mathbb{Q} -algebras E containing D which appear as endomorphism algebras of abelian surfaces. In other words, we would like to know which endomorphism algebra appears in the Shimura curve X_D associated to the quaternion algebra D (and with additional data). Our main result states as follows.

Theorem 1.1. *Let D be an indefinite quaternion division algebra over \mathbb{Q} , and let A be an abelian surface over a field k with quaternion multiplication by D , i.e. an abelian surface together with a \mathbb{Q} -algebra embedding $\iota : D \rightarrow E := \text{End}^0(A) := \text{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$.*

- (1) *Suppose that A is not simple. Then A is isogenous to C^2 for an elliptic curve C over k and the algebra E is isomorphic to one of the following*
 - (i) $\text{Mat}_2(K)$, where K is any imaginary quadratic field which splits D , or
 - (ii) $\text{Mat}_2(D_{p,\infty})$, where p is a prime and $D_{p,\infty}$ is the quaternion algebra over \mathbb{Q} ramified exactly at $\{p, \infty\}$. This occurs if and only if C is a supersingular elliptic curve over k with $k \supset \mathbb{F}_{p^2}$.
- (2) *Suppose that A is simple. Then we have*
 - (i) $E \simeq D$, or
 - (ii) $E \simeq D_K := D \otimes_{\mathbb{Q}} K$ for some imaginary quadratic field K . In this case, the abelian surface A is in characteristic $p > 0$ for some prime p and it is supersingular.

Recall that an abelian variety in characteristic $p > 0$ is said to be *supersingular* if it is isogenous to a product of supersingular elliptic curves over a finite field extension. The case (i) of Theorem 1.1 (2) occurs as we can take a generic complex abelian surface with QM by D . The case (ii) of Theorem 1.1 (2) occurs only when the quaternion algebra D satisfies a special condition and the simple abelian variety A is necessarily supersingular. In this case, the algebra E is obviously determined by its center K , and we show that there are only a finite list of possibilities for such K . More precisely, we have the following result.

Date: October 4, 2012.

2000 Mathematics Subject Classification. 11.

Key words and phrases. endomorphism algebras, QM abelian surfaces, quaternion algebras.

Theorem 1.2 (Theorem 2.11). *Let A be a simple supersingular abelian surface over a finite field \mathbb{F}_q of characteristic $p > 0$ with quaternion multiplication by D . Let $E := \text{End}^0(A)$ be the endomorphism algebra of A , and let S be the discriminant of D . Then*

- (1) *The center K of E is isomorphic to $\mathbb{Q}(\zeta_n)$ for $n = 3, 4$, or 6 .*
- (2) *One has $p \mid S$ and $p \equiv 1 \pmod{n}$, where n is as above, and for any other prime $\ell \mid S$, one has either $\ell \mid n$ or $\ell \equiv -1 \pmod{n}$, that is, ℓ does not split in the quadratic field $\mathbb{Q}(\zeta_n)$.*
- (3) *$E \simeq D \otimes_{\mathbb{Q}} K$.*

According to Theorem 1.2, there are three possibilities for endomorphism algebras E of simple supersingular abelian surfaces over finite fields: $E \simeq D \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_n)$ for $n = 3, 4, 6$. However, not all of them occur; It depends on the quaternion algebra D . The algebra $D \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_n)$ occurs if and only if there is exactly one prime p dividing S such that $p \equiv 1 \pmod{n}$ (This prime p is the characteristic of the base field).

The results of this paper (Theorems 1.1 and 1.2) contribute new cases to the problem about semi-simple algebras that can be realized as endomorphism algebras of abelian varieties. See Oort [9] and the references therein for quite complete discussions of this problem.

Supersingular abelian surfaces appear in the classification of endomorphism algebras of QM abelian surfaces. We refer the reader to C. Xing [19] for some aspects of supersingular abelian surfaces over finite fields.

Let J be the Jacobian of a smooth, projective, geometrically connected algebraic curve of genus 2 over a number field K . In [1] Baba and Granath showed that if the following three conditions hold: (1) J has QM by a maximal quaternion order Λ_6 of discriminant 6, (2) J has the field of moduli equal to \mathbb{Q} , and (3) J has potentially smooth stable reduction at both 2 and 3, then QM abelian surface J has superspecial good reduction at infinitely many primes. In [4] Dieulefait and Rotger studied the arithmetic of the Jacobians J whose endomorphism algebra $\text{End}_{\mathbb{Q}}^0(J)$ is an indefinite quaternion algebra. They determine all possible Galois groups of minimal fields of definition and possible endomorphism rings $\text{End}_K(J)$ defined over a smaller number field K under a certain integral condition. We refer the reader to [4] for the list of Galois groups and more detail discussions.

An analogous question to our main results (Theorems 1.1 and 1.2) is: What are the endomorphism algebras of abelian varieties with real multiplication (RM)? That is, one considers the same problem as treated in this paper but for Hilbert modular varieties rather than Shimura curves. This problem has been done by Chai [3, Section 3]. The classification has its own interest; this also plays a role in the proof of Chai's theorem on the density of ordinary Hecke orbits in Siegel modular varieties. As the reader may be also interested in this result due to Chai, we include an expository and elementary account for the reader's convenience in Section 3. Using the similar method as in Section 2, we make Chai's result more explicit about the simple algebras that actually occur as endomorphism algebras of RM abelian varieties.

2. PROOF OF MAIN RESULTS

2.1. Embeddings of simple algebras. We recall some basic definitions for central simple algebras; see [11].

Definition 2.1. Let B be a (f.d.) central simple algebra over a field F . The *degree*, *capacity*, and *index* of B are defined as

$$\deg(B) := \sqrt{[B : F]}, \quad c(B) := n, \quad i(B) := \sqrt{[\Delta : F]},$$

respectively, if $B \cong \text{Mat}_n(\Delta)$, where Δ is a division algebra over F , which is uniquely determined by B up to isomorphism. The algebra Δ is also called the *division part* of B .

Proposition 2.2. *Let E and B be two finite-dimensional simple algebras over a field F with centers Z and K , respectively. Suppose that Z and K are linearly disjoint over F , that is, the F -algebra $L := Z \otimes_F K$ is a field. Let $E \simeq \text{Mat}_n(\Delta)$, where Δ is the division part of E . Then there is an F -algebra embedding of B into E if and only if*

$$(2.1) \quad [B : F] \mid n \cdot c,$$

where c is the capacity of the central simple algebra $\Delta \otimes_F B^\circ$ over L :

$$\Delta \otimes_F B^\circ \simeq \Delta \otimes_Z (Z \otimes_F K) \otimes_K B^\circ \simeq (\Delta \otimes_Z L) \otimes_L (L \otimes_K B^\circ),$$

and B° denotes the opposite algebra of B .

PROOF. This is a special case of [18, Theorem 1.2]. However, instead of referring to the general result, we prefer to give a direct proof for the reader's convenience. Let $E = \text{End}_\Delta(V)$, where V is a right vector space over Δ . An F -algebra embedding from B into E exists if and only if V is a (B, Δ) -bimodule, or equivalently a right $\Delta \otimes_F B^\circ$ -module. Let $\Delta \otimes_F B^\circ \simeq \text{Mat}_c(\Delta')$, where Δ' is the division part of the simple algebra $\Delta \otimes_F B^\circ$. By the dimension counting, the vector space V is a $\text{Mat}_c(\Delta')$ -module if and only if

$$(2.2) \quad \frac{\dim_F V}{c[\Delta' : F]} \in \mathbb{N}.$$

Note that $[B : F][\Delta : F] = c^2[\Delta' : F]$. From this relation and that $\dim_F V = n[\Delta : F]$, the condition (2.2) can be written as $[B : F] \mid nc$. This proves the proposition. \blacksquare

Remark 2.3. The reader can find in [18] for more general results about Proposition 2.2 where B and E are any finite-dimensional semi-simple F -algebras. When F is a global field, the local-global principle enters and plays a role in the problem of embeddings of simple algebras. For a detailed discussion, the reader is referred to the paper [12].

After establishing a basic embedding result (Proposition 2.2), we begin with the classification of endomorphism algebras of QM abelian surfaces. Let (A, ι) be an abelian surface with quaternion multiplication by D and let $E := \text{End}^0(A) := \text{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ be the endomorphism algebra of A .

2.2. Case where A is not simple. In this case A is isogenous to $C_1 \times C_2$, where C_1 and C_2 are elliptic curves. Then C_1 is isogenous to C_2 . If not, then we have inclusions $D \subset \text{End}^0(C_i)$ for $i = 1, 2$ and each C_i must be supersingular. It follows that $D \simeq \text{End}^0(C_i) \simeq D_{p,\infty}$, the definite quaternion algebra over \mathbb{Q} ramified exactly at $\{p, \infty\}$, contradiction.

Therefore, the algebra $E = \text{End}^0(A) = \text{End}(A) \otimes \mathbb{Q}$ is isomorphic to one the following:

- (i) $\text{Mat}_2(\mathbb{Q})$,
- (ii) $\text{Mat}_2(K)$, where K is an imaginary quadratic field,
- (iii) $\text{Mat}_2(D_{p,\infty})$.

The case (i) can not occur because D and $\text{Mat}_2(\mathbb{Q})$ are different quaternion algebras.

The case (ii) can appear if and only if K splits D . Indeed, as one has an embedding of D in $\text{Mat}_2(K)$, the algebra D acts on a K -vector space V of dimension two. We can identify V with D as V is one-dimensional D -vector space. This makes D a K -vector space of dimension 2. Therefore, K is isomorphic to a (necessarily) maximal subfield of D . This is exactly when K splits D . On the other hand, any imaginary quadratic field is isomorphic to the endomorphism algebra of an elliptic curve. Therefore, for any imaginary quadratic field that splits D , the matrix algebra $\text{Mat}_2(K)$ can occur as the endomorphism algebra of a QM abelian surface.

For the case (iii), this occurs of course only when A is in characteristic $p > 0$ and A is isogenous to the product of two supersingular elliptic curves over the base field k containing \mathbb{F}_{p^2} . Now we check that an embedding $\iota : D \rightarrow \text{Mat}_2(D_{p,\infty})$ exists for any prime p . By Proposition 2.2, we need to show that $[D : \mathbb{Q}] \mid 2c$, where c is the capacity of the central simple algebra $D^\circ \otimes_{\mathbb{Q}} D_{p,\infty}$ over \mathbb{Q} and D° denotes the opposite algebra of D . As the tensor product of two quaternion algebras is Brauer equivalent to a quaternion algebra, we have

$$D^\circ \otimes_{\mathbb{Q}} D_{p,\infty} \simeq \text{Mat}_2(D')$$

for some definite quaternion algebra D' over \mathbb{Q} . This shows that $c = 2$ and hence that a \mathbb{Q} -algebra embedding $\iota : D \rightarrow \text{Mat}_2(D_{p,\infty})$ exists. We have shown the following result.

Proposition 2.4. *Let D be as above and A be an abelian surface with endomorphism algebra $E := \text{End}^0(A)$ containing D . Suppose that A is not simple. Then A is isogenous to C^2 for an elliptic curve C and the algebra E is isomorphic to one of the following two cases*

- (i) $\text{Mat}_2(K)$, where K is any imaginary quadratic field which splits D , or
- (ii) $\text{Mat}_2(D_{p,\infty})$. This occurs if and only if C is a supersingular elliptic curve in characteristic $p > 0$ and the base field k contains \mathbb{F}_{p^2} .

2.3. Case where A is simple. Since $E := \text{End}^0(A)$ contains the quaternion algebra D , the algebra E is non-commutative. Let K be the center of E . Since $\dim A = 2$, any maximal subfield of E has degree 2 or 4 (over \mathbb{Q}). So one has $[K : \mathbb{Q}] \mid 4$. If $[K : \mathbb{Q}] = 4$, then $E = K$ (which is commutative), absurd. So $K = \mathbb{Q}$ or $[K : \mathbb{Q}] = 2$.

If $K = \mathbb{Q}$, which is totally real, then E is a quaternion algebra over \mathbb{Q} . This follows from Albert's classification of central division algebras with positive involution (cf. Mumford [6, Section 21]). In this case, one must have $E \simeq D$.

Suppose now that $[K : \mathbb{Q}] = 2$. Then E is a quaternion division algebra over K . If K is real, then $E \supset D \otimes_{\mathbb{Q}} K$ contains a totally real maximal subfield K' (of degree 4 over \mathbb{Q}), which shows that $\dim A$ is divisible by 4 (see Mumford [6, Corollary, p. 191]), absurd. It follows that the center K is an imaginary quadratic field. Note that in this case, A is in characteristic $p > 0$ for some prime p . Indeed, its endomorphism algebra contains a 4-dimensional CM subfield. We also know that any simple CM abelian variety by a CM field L in characteristic zero has endomorphism algebra equal to L but E is non-commutative. Therefore, A is in positive characteristic. Now we determine which quaternion division algebra E over an imaginary quadratic field K contains a subalgebra isomorphic to D . This is exactly when the capacity of $E \otimes_{\mathbb{Q}} D^\circ$ is equal to 4 by Proposition 2.2, or equivalently, the quaternion algebra $D_K := D \otimes_{\mathbb{Q}} K$ is isomorphic to E . We have shown the following result.

Proposition 2.5. *Let D be as above and A be an abelian surface with quaternion multiplication by D . Suppose that A is simple. Then*

- (i) $E \simeq D$, or
- (ii) $E \simeq D_K := D \otimes_{\mathbb{Q}} K$ for some imaginary quadratic field K . In this case, the abelian surface A is in characteristic $p > 0$ for some prime p .

Theorem 1.1 follows from Propositions 2.4 and 2.5.

The case (i) of Proposition 2.5 occurs as one can take A to be a generic complex QM abelian surface. For the case (ii), we make a further discussion about the algebras of the form D_K that can occur in the next subsection.

2.4. Put $D_K := D \otimes_{\mathbb{Q}} K$, where K is an imaginary quadratic field. In the remaining of this section, we investigate which D_K can be realized as the endomorphism algebra of an abelian surface.

Suppose $D_K \simeq \text{End}^0(A)$ for an abelian surface. Then A has smCM (sufficiently many complex multiplications, that is, the endomorphism algebra $\text{End}^0(A)$ of A contains a semi-simple commutative \mathbb{Q} -subalgebra L with $[L : \mathbb{Q}] = 2 \dim A$). By a theorem of Grothendieck [6, Section 22, p. 220], there are a finite field extension k' of the ground field k and an abelian surface A_0 over a finite field k_0 contained in k' such that there is an isogeny $A \otimes_k k' \rightarrow A_0 \otimes_{k_0} k'$ over k' (see [7] for Grothendieck's original proof and [16] for a different proof). We may enlarge k_0 in k' , if necessary, such that $\text{End}^0(A_0 \otimes_{k_0} k') = \text{End}_{k_0}^0(A_0) =: E_0$. This shows the following:

Lemma 2.6. *Notations being as above, the algebra $E \simeq D_K$ is contained in the endomorphism algebra E_0 of an abelian surface over a finite field.*

Since $[E : \mathbb{Q}] = 8$, one has either

- (a) $E = E_0$, or
- (b) $\dim E_0 = 16$.

Lemma 2.7. *Let notations be as above. For either the case (a) or (b), there is a rational prime p which splits in K . Furthermore we have for any finite place v of*

K

$$(2.3) \quad \text{inv}_v(E) = \begin{cases} 1/2 & \text{if } v|p, \\ 0 & \text{otherwise.} \end{cases}$$

PROOF. For the case **(b)**, the algebra $E_0 \simeq \text{Mat}_2(D_{p,\infty})$ for some rational prime p . The algebra D_K can be embedded in E_0 if and only if $D_{p,\infty} \otimes_{\mathbb{Q}} K \simeq D_K \simeq E$. Since $\text{inv}_{\infty}(E) = 0$ and E is a division algebra, the places with non-trivial invariants are those of K over p . It follows that there are two places of K lying over p at which E has non-trivial local invariant, and the remaining local invariants are trivial.

For the case **(a)**, E is the endomorphism algebra of an abelian surface A_0 over a finite field k_0 . Using the Honda-Tate theory, the center K is $\mathbb{Q}(\pi_0)$, where π_0 is the relative Frobenius endomorphism of A_0 over k_0 . For any finite place v of K with $v \nmid p$, one has $\text{inv}_v(E) = 0$. As E is a division algebra, it follows that there are two places of K lying over p at which E has non-trivial local invariant, and the remaining local invariants are trivial. ■

We need to find all rational primes p and imaginary quadratic fields K such that the quaternion algebra $D_K := D \otimes_{\mathbb{Q}} K \simeq E$ satisfies the condition of Lemma 2.7 and that the algebra E appears as the endomorphism algebra of an abelian surface. Let S be the discriminant of D over \mathbb{Q} ; by definition, S is the product of all finite ramified rational primes for D . Clearly, one has $p \mid S$, otherwise the local invariants of D_K at places v lying over p are zero and hence that $D_K \simeq \text{Mat}_2(K)$, absurd. Therefore, a necessary condition that K satisfies the conditions in Lemma 2.7 is the following:

(*) The prime p splits in K and for any other prime $\ell \mid S$, the completion $K_{\ell} := K \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell}$ at ℓ is a field.

The first condition of (*) follows from $\text{inv}_v(E) = 1/2$ if $v|p$ and the second one follows from $\text{inv}_v(E) = 0$ otherwise.

Now given a rational prime $p \mid S$ and an imaginary quadratic field K satisfying the condition (*), we would like to find a Weil q -number π , where q is a power of p , so that $K \simeq \mathbb{Q}(\pi)$ and for every place $v \mid p$ of K , one has $v(\pi)/v(q) = 1/2$.

Lemma 2.8. *Let (A, ι) be an abelian surface with QM by D over a field k of characteristic $p > 0$. Suppose that $p \mid S$, then A is supersingular.*

PROOF. This result is well-known (see [2]); we provide a proof for the reader's convenience. We may assume that the ground field k is algebraically closed. We have a \mathbb{Q}_p -algebra embedding $\iota : D_p := D \otimes_{\mathbb{Q}} \mathbb{Q}_p \rightarrow \text{End}^0(X)$, where $X := A[p^{\infty}]$ is the p -divisible group attached to A . The possibilities of $\text{End}^0(X)$ are (a) (ordinary) $\text{Mat}_2(\mathbb{Q}_p) \times \text{Mat}_2(\mathbb{Q}_p)$, (b) (p -rank one) $D_p \times \mathbb{Q}_p \times \mathbb{Q}_p$, and (c) (supersingular) $\text{Mat}_2(D_p)$. Clearly, only the case (c) is possible. Therefore, the abelian surface A is supersingular. ■

We need to find all Weil q -numbers π so that the corresponding abelian variety A_{π} , uniquely determined up to isogeny, is both simple and supersingular, and that its center $\mathbb{Q}(\pi)$ is an imaginary quadratic field satisfying the condition (*). The latter condition will imply that the endomorphism algebra of A_{π} is a quaternion division algebra over K and hence that A_{π} is an abelian surface.

Theorem 2.9. *Let q be a power of a prime number p and π is a Weil q -number. Then the corresponding abelian variety A_π is supersingular if and only if $\pi = \sqrt{q}\zeta$, where ζ is a root of unity.*

PROOF. This is a well-known immediate consequence of results due to Manin [5], Tate [14] and Oort [8, Theorem 2], also see [19]. We provide a proof for the reader's convenience. Let C be a supersingular elliptic curve over \mathbb{F}_p such that $\pi_C^2 + p = 0$, where π_C is the Frobenius endomorphism of C/\mathbb{F}_p . Put $A_1 = C^g$, where $g = \dim A_\pi$. Since any two supersingular abelian varieties are isogenous over a finite extension of their ground fields, we have $\pi^N = p^M$ for some positive integers N and M . It follows that π is of the form $\sqrt{q}\zeta$, where ζ is a root of unity. Conversely, suppose that π is of this form. Then π^N , for some even integer N , is $q^{N/2}$, which is a Weil number corresponding to a supersingular elliptic curve. By Tate's isogeny theorem, A is isogenous to the product of copies of a supersingular elliptic curve over a finite field. This completes the proof of the theorem. ■

We shall call a Weil q -number π *supersingular* if the corresponding simple abelian variety A_π up to isogeny is supersingular.

Lemma 2.10. *Let $\pi = \sqrt{q}\zeta_n$ be a supersingular Weil q -number, where $q = p^a$, and ζ_n is a primitive n -th root of unity. Then the field $K = \mathbb{Q}(\pi)$ generated by π is an imaginary quadratic field if and only if*

- (a) a is even and $n = 3, 4, 6$, or
- (b) a is odd and $n = 4$.

PROOF. (a) One has $\mathbb{Q}(\pi) = \mathbb{Q}(\zeta_n)$, so $[\mathbb{Q}(\pi) : \mathbb{Q}] = 2$ if and only if $n = 3, 4, 6$. (b) The map $\sigma : \pi \mapsto -\pi$ induces a non-trivial field automorphism of $\mathbb{Q}(\pi)$, therefore $[\mathbb{Q}(\pi) : \mathbb{Q}(\pi^2)] = 2$. So the field $\mathbb{Q}(\pi^2) = \mathbb{Q}(\zeta_n^2)$ must be equal to \mathbb{Q} . This is the case only when $n = 4$. ■

Note that in the case (a) the prime p splits in $\mathbb{Q}(\pi)$ if and only if $p \equiv 1 \pmod{n}$. In the case (b) p is ramified in $\mathbb{Q}(\pi)$. Therefore, if one requires the field $\mathbb{Q}(\pi)$ satisfy the condition (*), then only the case (a) can occur. This yields the following conclusion.

Theorem 2.11. *Let A be a simple supersingular abelian surface over a finite field \mathbb{F}_q of characteristic $p > 0$ with quaternion multiplication by D and let $E := \text{End}^0(A)$. Then*

- (1) *The center K of E is isomorphic to $\mathbb{Q}(\zeta_n)$ for $n = 3, 4$, or 6 .*
- (2) *One has $p \mid S$ and $p \equiv 1 \pmod{n}$, where n is as above, and for any other prime $\ell \mid S$, one has either $\ell \nmid n$ or $\ell \equiv -1 \pmod{n}$.*
- (3) *$E \simeq D \otimes_{\mathbb{Q}} K$.*

It follows from Theorem 2.11 that there are three possibilities for endomorphism algebras E of simple supersingular abelian surfaces over finite fields: $E \simeq D \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_n)$ for $n = 3, 4, 6$. Furthermore, the algebra $D \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_n)$ occurs if and only if there is exactly one prime $p \mid S$ such that $p \equiv 1 \pmod{n}$. This prime is the characteristic of the ground field of the abelian surface.

We conclude this section with a remark and a question we think interesting. Let E be the endomorphism algebra of a simple QM abelian surface A such that $E \neq D$. Then

- A is in characteristic $p > 0$ for a prime p , and A is supersingular,
- $E = D \otimes_{\mathbb{Q}} K$, where K is an imaginary quadratic field satisfying the condition (*) after Lemma 2.7.
- In case that E is isomorphic to the endomorphism algebra of supersingular simple QM abelian surface over a finite field, we know all such K that can occur by Theorem 2.11.

However, we are not able to rule out the possibility that E is not isomorphic to a (necessarily supersingular) simple QM abelian surface over a *finite field*. That is, whether or not the endomorphism algebra of any supersingular abelian surface over an *arbitrary field* k is isomorphic to that of one over a finite field. We make the following hypothesis.

(H) Let k , k' and k_0 be three fields with the inclusion relation $k \subset k' \supset k_0$. Let A/k and A_0/k_0 be two abelian varieties such that there is an isogeny $\varphi : A \otimes_k k' \rightarrow A_0 \otimes_{k_0} k'$ over k' . Suppose that $\text{End}^0(A_0) = \text{End}^0(A_0 \otimes_{k_0} k')$. We identify $\text{End}^0(A \otimes_k k') = \text{End}^0(A_0)$ using the isogeny φ . Then there is an abelian variety A_1/k_1 over a subfield $k_1 \subset k_0$ and an isogeny $\varphi_1 : A_1 \otimes_{k_1} k_0 \rightarrow A_0$ over k_0 so that the subalgebra $\text{End}^0(A_1) \subset \text{End}^0(A_0)$ (through φ_1) is equal to the subalgebra $\text{End}^0(A)$ in $\text{End}^0(A \otimes_k k') = \text{End}^0(A_0)$.

The hypothesis **(H)** rules out the possibility of imaginary quadratic fields K satisfying the necessary condition (*) that are not of the shape described in Theorem 2.11. Then Theorems 1.1 and 1.2 give a complete result for endomorphism algebras of QM abelian surfaces over an arbitrary base field. Besides, we also obtain the following result, which is an immediate consequence of a theorem of Grothendieck (cf. [7], [16]).

Corollary 2.12. *Let A/k be an abelian variety that has smCM over a field k of characteristic $p > 0$. Assume the hypothesis **(H)**. Then the endomorphism algebra $\text{End}^0(A)$ of A/k is isomorphic to that of an abelian variety over a finite field.*

Even when the hypothesis **(H)** fails, one is still in an interesting situation. This means there are some subtle issues about the fields of definition that we were not aware of. For example, there are endomorphism algebras of abelian varieties having smCM in positive characteristic that can not be found by the Honda-Tate theory. These would contribute new examples to the problem of endomorphism algebras of abelian varieties studied in Oort [9].

The following question should be helpful to understand the problem of fields of definition arising from **(H)**. Recall that an abelian variety over a field k of characteristic $p > 0$ is said to be *superspecial* if it is isomorphic to a product of supersingular elliptic curves over an algebraic closure of k .

(Q). Let A be a superspecial abelian variety over a field k of characteristic $p > 0$. Is there a superspecial abelian variety A_0 over a finite field k_0 so that A is isomorphic to $A_0 \otimes_{k_0} k$ over k ?

3. ENDOMORPHISM ALGEBRAS OF RM ABELIAN VARIETIES

In this section, we give an exposition on endomorphism algebras of abelian varieties with real multiplication. Our reference is Chai [3], especially Section 3 of it. The classification has its own interest; this is also useful in the proof of Chai's theorem on the density of ordinary Hecke orbits in Siegel modular varieties. We change the notations a bit. Let F be a totally real number field of degree $g = [F : \mathbb{Q}]$, and let O_F be the ring of integers. An *abelian variety with real multiplication by O_F* is a pair (A, ι) , where A is a g -dimensional abelian variety and $\iota : O_F \rightarrow \text{End}(A)$ is a ring monomorphism. As we are only concerned with the endomorphism algebra $\text{End}^0(A)$ of such objects, we may replace the ring monomorphism $\iota : O_F \rightarrow \text{End}(A)$ by its induced \mathbb{Q} -algebra embedding $\iota : F \rightarrow \text{End}^0(A)$. We shall call the latter object (A, ι) an *abelian variety with RM by F* .

Let (A, ι) be an abelian variety with RM by F over an (unspecified) base field k .

Lemma 3.1. *The underlying abelian variety A is isogenous to A_1^n , where A_1 is a simple abelian variety.*

PROOF. Let A be isogenous to $\prod_{j=1}^r A_j^{n_j}$, where A_i and A_j are non-isogenous simple abelian varieties if $i \neq j$. Then one has a \mathbb{Q} -algebra embedding $\iota : F \rightarrow \text{End}^0(A_j^{n_j})$ for each $j = 1, \dots, r$, and hence $g \mid \dim A_j^{n_j}$. It follows that $r = 1$. ■

Put $d := \dim A_1$ and $\Delta := \text{End}^0(A_1)$. One has $g = nd$ and $\text{End}^0(A) = \text{Mat}_n(\Delta)$. The division algebra Δ admits a positive (Rosati) involution $*$. We use the classification of Albert for Δ (cf. [6, Section 21]).

(Type I) The algebra $\Delta = K_0$ is a totally real number field. Since $F \simeq \iota(F) \subset \text{Mat}_n(K_0)$, one has $g \mid n[K_0 : \mathbb{Q}]$. On the other hand, one has $[K_0 : \mathbb{Q}] \mid d$. It follows that $d = [K_0 : \mathbb{Q}]$. The map ι makes the K_0 -vector space $V = K_0^n$ as an F -vector space of dimension one. Therefore, F can be regraded as a K_0 -vector space and hence K_0 is isomorphic to a subfield of F . We may assume that K_0 is a subfield of F . Conversely, given a subfield K_0 of F of degree d , we choose an abelian variety A_1 so that the endomorphism algebra $\text{End}^0(A_1)$ is isomorphic to K_0 . Take $A := A_1^n$, where $n := g/d$. Since there is a \mathbb{Q} -algebra embedding $\iota : F \rightarrow \text{Mat}_n(K_0)$, we have an abelian variety (A, ι) with RM by F such that $\text{End}^0(A)$ is isomorphic to $\text{Mat}_n(K_0)$.

(Type II) The algebra Δ is a totally indefinite quaternion algebra over a totally real number field K_0 . Since Δ contains a totally real maximal subfield K_1 , which has degree $2[K_0 : \mathbb{Q}]$, one has $2[K_0 : \mathbb{Q}] \mid \dim A_1$. On the other hand, any maximal subfield of $\text{Mat}_n(\Delta)$ has degree $2n[K_0 : \mathbb{Q}]$, which gives the other divisibility $g \mid 2n[K_0 : \mathbb{Q}]$. Therefore, we have $g = 2n[K_0 : \mathbb{Q}]$ and $\dim A_1 = 2[K_0 : \mathbb{Q}]$. Since F has the degree of maximal semi-simple commutative subalgebras of $\text{Mat}_n(\Delta)$, the image of any embedding ι contains the center K_0 . Therefore, we may assume that K_0 is a subfield of F and ι is a K_0 -algebra embedding of F into $\text{Mat}_n(\Delta)$. The field F is isomorphic to a (maximal) subfield of $\text{Mat}_n(\Delta)$ if and only if F splits Δ . The latter is equivalent to that for any place $v \in \text{Ram}(\Delta/K_0)$, the set of ramified places of K_0 for Δ , and any place $w \nmid v$ of F , one has $[F_w : K_{0,v}] \equiv 0 \pmod{2}$.

Conversely, suppose we have a subfield K_0 of F with $2[K_0 : \mathbb{Q}]n = g$ for some positive integer n , and a totally indefinite quaternion algebra Δ over K_0 which is split by F . Then there exists an abelian variety with RM by F so that $\text{End}^0(A) \simeq \text{Mat}_n(\Delta)$. Indeed, we first take a complex abelian variety A_1 with dimension $2[K_0 : \mathbb{Q}]$ so that $\text{End}^0(A_1) \simeq \Delta$. Then put $A := A_1^n$. The condition that F splits Δ implies that there is a K_0 -algebra embedding from F into $\text{Mat}_n(\Delta)$. This way we construct a (complex) abelian variety with RM by F so that $\text{End}^0(A) \simeq \text{Mat}_n(\Delta)$.

(Type III) The algebra Δ is a totally definite quaternion algebra over a totally real number field K_0 . Since F can be embedded in $\text{Mat}_n(\Delta)$, whose maximal semi-simple commutative subalgebras have the same degree $2n[K_0 : \mathbb{Q}]$, one has $g|2n[K_0 : \mathbb{Q}]$. On the other hand, as the field K_0 acts on the abelian variety A_1 up to isogeny, one has $[K_0 : \mathbb{Q}]|\dim A_1$; this gives the condition $n[K_0 : \mathbb{Q}]|g$. Also, if the ground field k is of characteristic zero, then the algebra Δ acts on the homology group $H_1(A_1, \mathbb{Q})$. This gives the condition $4[K_0 : \mathbb{Q}]|2\dim A_1$, or equivalently $2n[K_0 : \mathbb{Q}]|g$. We have two cases:

- (a) $g = n[K_0 : \mathbb{Q}]$. This case occurs only when k is of characteristic $p > 0$ for some prime p .
- (b) $g = 2n[K_0 : \mathbb{Q}]$.

We first rule out the possibility of (b). Since g is the degree of any maximal semi-simple commutative subalgebra of $\text{Mat}_n(\Delta)$, the image of F under any embedding $\iota : F \rightarrow \text{Mat}_n(\Delta)$ contains the center K_0 . Therefore, F contains a subfield which is isomorphic to K_0 , and we may assume that the field F contains K_0 and the embedding ι is a K_0 -algebra homomorphism. Since F has the degree of $\text{Mat}_n(\Delta)$ over K_0 , the field F can be embedded into the simple algebra $\text{Mat}_n(\Delta)$ if and only if F splits Δ . But the latter is impossible because Δ is totally definite and F is totally real.

For the case (a), we have $\dim A_1 = [K_0 : \mathbb{Q}]$. In this case the abelian variety A_1 has smCM. By a theorem of Grothendieck [6, Section 22, p. 220], there are a finite field extension k'/k , an abelian variety A_0 over a finite field k_0 contained in k' and an isogeny $\varphi : A_1 \otimes_k k' \rightarrow A_0 \otimes_{k_0} k'$. Enlarging k_0 if necessary, we can assume that $\text{End}^0(A_0 \otimes_{k_0} k') = \text{End}^0(A_0)$. We have

$$\Delta = \text{End}^0(A_1) \subset \text{End}^0(A_1 \otimes_k k') \simeq \text{End}^0(A_0 \otimes_{k_0} k') = \text{End}^0(A_0).$$

We first show that A_0 (and A_1) is supersingular. We know that both Δ and $\text{End}^0(A_0)$ have the same degree ($=2\dim A_1$) of maximal semi-simple commutative subalgebras. The centralizer of K_0 of $\text{End}^0(A_0)$ is equal to the division algebra Δ and hence by bi-commutant theorem [11, Theorem 7.11 and Corollary 7.13, p. 94-95] that the centralizer of Δ in $\text{End}^0(A_0)$ is equal to K_0 . It follows that the center Z of $\text{End}^0(A_0)$ is contained in the totally real field K_0 . By the classification of endomorphism algebras of abelian varieties over finite fields in Tate [13], the field Z is equal to \mathbb{Q} or $\mathbb{Q}(\sqrt{p})$ and A_0 is supersingular. We may enlarge the field k_0 so that A_0 is isogenous to the product of copies of supersingular elliptic curves with endomorphism algebra $D_{p,\infty}$. Therefore, $\text{End}^0(A_0) = \text{Mat}_{[K_0:\mathbb{Q}]}(D_{p,\infty})$, noting that $\dim A_0 = \dim A_1 = g/n = [K_0 : \mathbb{Q}]$. Then the division algebra Δ is equal to the centralizer of K_0 in $\text{Mat}_{[K_0:\mathbb{Q}]}(D_{p,\infty})$. It follows that Δ is ramified

exactly at all Archimedean places and finite places v of K_0 over p of odd degree, or equivalently $\Delta \simeq D_{p,\infty} \otimes_{\mathbb{Q}} K_0$. If we assume the hypothesis **(H)** (at the end of Section 2), then there are only two possibilities for Δ : either $\Delta = D_{p,\infty}$ or $\Delta = D_{\infty_1,\infty_2}$, the definite quaternion algebra over the field $\mathbb{Q}(\sqrt{p})$ which is ramified exactly at two Archimedean places ∞_1 and ∞_2 . We have given all possibilities of the division algebras Δ , and only the cases $\Delta = D_{p,\infty}$ and $\Delta = D_{\infty_1,\infty_2}$ can occur as endomorphism algebras of simple abelian varieties over finite fields.

We now show that the field F contains a subfield which is isomorphic to K_0 , so that we may assume that F contains K_0 and that the embedding ι is a K_0 -algebra homomorphism. Let $x \mapsto \bar{x}$ be the canonical involution of Δ , which is the unique positive involution. Define a positive involution $*$ on $\text{Mat}_n(\Delta)$ by $(a_{ij})^* = (\bar{a}_{ji})$. We know that for any embedding $\iota : F \rightarrow \text{Mat}_n(\Delta)$, there is a positive involution $*_1$ which leaves the image $\iota(F)$ invariant and every element of $\iota(F)$ invariant. On the other hand, one can show that there is an isomorphism of algebras with involution $(\text{Mat}_n(\Delta), *_1) \simeq (\text{Mat}_n(\Delta), *)$. This follows from the Noether-Skolem theorem, the fact that the unitary group $U(\text{Mat}_n(\Delta), *)$ is semi-simple and simply-connected, and the Kneser theorem on the H^1 -vanishing for simply-connected groups over non-Archimedean local fields. For the details of this argument, see for example [17, Section 2]. Therefore, we may assume that the image of F is fixed by $*$. Since the maximal semi-simple commutative subalgebras of $\text{Mat}_n(\Delta)$ stable by the involution has degree $n[K_0 : \mathbb{Q}]$ over \mathbb{Q} , the image $\iota(F)$ contains the center K_0 . This shows that F contains a subfield that is isomorphic to K_0 .

As $[F : K_0] = n$, a K_0 -algebra embedding $\iota : F \rightarrow \text{Mat}_n(\Delta)$ always exists if Δ is the endomorphism algebra of a simple abelian variety A_1 of dimension $[K_0 : \mathbb{Q}]$. The abelian variety $(A = A_1^n, \iota)$ with RM by F has endomorphism algebra $\text{End}^0(A) \simeq \text{Mat}_n(\Delta)$.

(Type IV) The algebra Δ is a central simple algebra over a CM field K with maximal real number field K_0 . For any finite place v of K , one has

$$(3.1) \quad \text{inv}_v(\Delta) + \text{inv}_{\sigma(v)}(\Delta) = 0, \quad \text{and} \quad \text{inv}_v(\Delta) = 0 \quad \text{if} \quad \sigma(v) = v,$$

where σ is the non-trivial automorphism of K/K_0 . This is the necessary and sufficient condition for the central simple Δ that admits a positive involution. Let $m := \deg(\Delta)$. The algebra Δ contains a (maximal) totally real subfield F' of degree $m[K_0 : \mathbb{Q}]$ over \mathbb{Q} , therefore one has $m[K_0 : \mathbb{Q}] \mid \dim A_1$, or equivalently $nm[K_0 : \mathbb{Q}] \mid g$. On the other hand, since the field F can be embedded into $\text{Mat}_n(\Delta)$, one has the condition $g \mid nm[K_0 : \mathbb{Q}]$. This shows $\dim A_1 = m[K_0 : \mathbb{Q}]$ and A_1 has smCM. Since any maximal semi-simple commutative subalgebra of $\text{Mat}_n(\Delta)$ that is stable for a positive involution has degree $nm[K_0 : \mathbb{Q}]$, which is also equal to $[F : \mathbb{Q}]$, the image $\iota(F)$ contains a subfield which is isomorphic to K_0 . Therefore, we may assume that F contains K_0 and that the embedding map ι is a K_0 -algebra homomorphism.

We now determine the condition for Δ so that the totally real field F can be embedded into $\text{Mat}_n(\Delta)$ over K_0 . Note that $[F : K_0] = \deg(\text{Mat}_n(\Delta)/K)$. Put $L = F \otimes_{K_0} K$. The CM field L is isomorphic to a maximal subfield of $\text{Mat}_n(\Delta)$. The local-global principle (cf. [10, Theorem A.1] and [18]) asserts that this holds if and only if for any (finite) ramified place v of K for Δ , one has $[L_w : K_v] \cdot \text{inv}_v(\Delta) \in \mathbb{Z}$. If v is fixed by σ , then $\text{inv}_v(\Delta) = 0$ and hence the condition is satisfied automatically.

Let v be a finite ramified place of K and v_0 be the place of K_0 below v ; the place v_0 splits in K . For any place w_0 of F lying over v_0 , one also has that w_0 splits in L . Therefore $[F_{w_0} : K_{0,v_0}] = [L_w : K_v]$, where w is any place of L over w_0 . One concludes that the field F can be embedded into $\text{Mat}_n(\Delta)$ over K_0 if and only if for any (finite) ramified place v of K for Δ (note: $\sigma(v) \neq v$),

$$(3.2) \quad [F_{w_0} : K_{0,v_0}] \cdot \text{inv}_v(\Delta) = 0 \quad (\text{in } \mathbb{Q}/\mathbb{Z}), \quad \forall w_0|v_0.$$

Conversely, suppose we are given a central division algebra Δ over a CM field K with maximal totally real field K_0 that satisfies the local condition (3.1). Suppose also that (1) K_0 is contained in F , (2) $m[K_0 : \mathbb{Q}] = [F : \mathbb{Q}]$, where $m = \deg(\Delta/K)$, and (3) the condition (3.2) is satisfied. Then there is an abelian variety (A, ι) with RM by F such that $\text{End}^0(A) \simeq \text{Mat}_n(\Delta)$. Indeed, we take a complex abelian variety A_1 of dimension $m[K_0 : \mathbb{Q}]$ such that $\text{End}^0(A_1) \simeq \Delta$. Above discussion shows that there is a K_0 -algebra embedding $\iota : F \rightarrow \text{Mat}_n(\Delta)$. Set $A := A_1^n$, then the pair (A, ι) has the desired property.

We summarize the classification in the following theorem. This is a result of Chai [3, Lemma 6], while we make it more explicit about simple algebras that can actually occur as endomorphism algebras of RM abelian varieties over more general (unspecified) ground fields.

Theorem 3.2. *Let (A, ι) be a g -dimensional abelian variety with RM by F over a field k . Then $\text{End}^0(A) \simeq \text{Mat}_n(\Delta)$ for a positive integer n and a division algebra Δ .*

(Type I) *The algebra $\Delta = K_0$ is a totally real number field. Then the field K_0 can be embedded as a subfield in F with $n[K_0 : \mathbb{Q}] = g$.*

Conversely, given a subfield K_0 of F of degree d , then there is an abelian variety (A, ι) with RM by F such that $\text{End}^0(A) \simeq \text{Mat}_n(K_0)$, where $n := g/d$.

(Type II) *The algebra Δ is a totally indefinite quaternion algebra over a totally real number field K_0 . Then the field K_0 can be embedded as a subfield of F with $2n[K_0 : \mathbb{Q}] = g$ and F splits the quaternion algebra Δ .*

Conversely, given a subfield K_0 of F with $2n[K_0 : \mathbb{Q}] = g$ for some positive integer n , and Δ an indefinite quaternion algebra over K_0 such that F splits Δ . Then there is an abelian variety (A, ι) with RM by F such that $\text{End}^0(A) \simeq \text{Mat}_n(\Delta)$.

(Type III) *The algebra Δ is a totally definite quaternion algebra over a totally real number field K_0 . Then the field K_0 can be embedded as a subfield of F with $n[K_0 : \mathbb{Q}] = g$. The characteristic of the base field k is a prime $p > 0$, and A is supersingular. Moreover, we have $\Delta \simeq D_{p,\infty} \otimes_{\mathbb{Q}} K_0$. Under the assumption of the hypothesis (H), we have $\Delta \simeq D_{p,\infty}$ with $K_0 = \mathbb{Q}$, or D_{∞_1, ∞_2} with $K_0 = \mathbb{Q}(\sqrt{p})$.*

Conversely, suppose (Δ, K_0) is one of the above two cases and suppose that K_0 is contained in F . Then there exists an abelian variety (A, ι) with RM by F over a finite field such that $\text{End}^0(A) \simeq \text{Mat}_n(\Delta)$, where $n = g/[K_0 : \mathbb{Q}]$.

(Type IV) *The algebra Δ is a central simple algebra over a CM field K with maximal real number field K_0 . Then the field K_0 can be embedded in F with $g = nm[K_0 : \mathbb{Q}]$*

where $m = \deg(\Delta/K)$. For any finite ramified place v of K for Δ , we have

$$(3.3) \quad [F_{w_0} : K_{0,v_0}] \cdot \text{inv}_v(\Delta) = 0 \quad (\text{in } \mathbb{Q}/\mathbb{Z}), \quad \forall w_0|v_0,$$

where v_0 is the place of K_0 below v .

Conversely, let Δ be a central division algebra over a CM field K with maximal totally real field K_0 that admits a positive involution. Suppose that (1) K_0 is contained in F , (2) $mn[K_0 : \mathbb{Q}] = [F : \mathbb{Q}]$ for some positive integer n , where $m = \deg(\Delta/K)$, and (3) the condition (3.3) is satisfied. Then there is an abelian variety (A, ι) with RM by F such that $\text{End}^0(A) \simeq \text{Mat}_n(\Delta)$.

ACKNOWLEDGMENTS

The author thanks C.-L. Chai for his constant support and encouragement, as well as his work [3] where the second part of this paper is based on. The author was partially supported by grants NSC 100-2628-M-001-006-MY4 and AS-99-CDA-M01. Finally he thanks the referee for helpful suggestions on the organization that improve the presentation of this paper.

REFERENCES

- [1] S. Baba and H. Granath, Primes of superspecial reduction for QM abelian surfaces. *Bull. London Math. Soc.* **40** (2008), no. 2, 311–318.
- [2] J.-F. Boutot and H. Carayol, Uniformisation p-adique des courbes de Shimura: les théorèmes de Čerednik et de Drinfel'd. *Courbes modulaires et courbes de Shimura* (Orsay, 1987/1988). *Astérisque* No. **196-197** (1991), 45–158.
- [3] C.-L. Chai, Every ordinary symplectic isogeny class in positive characteristic is dense in the moduli. *Invent. Math.* **121** (1995), 439–479.
- [4] L. Dieulefait and V. Rotger, The arithmetic of QM-abelian surfaces through their Galois representations. *J. Algebra* **281** (2004), no. 1, 124–143.
- [5] Yu. Manin, Theory of commutative formal groups over fields of finite characteristic. *Russian Math. Surveys* **18** (1963), 1–80.
- [6] D. Mumford, *Abelian Varieties*. Oxford University Press, 1974.
- [7] F. Oort, The isogeny class of a CM-type abelian variety is defined over a finite extension of the prime field. *J. Pure Appl. Algebra* **3** (1973), 399–408.
- [8] F. Oort, Which abelian surfaces are products of elliptic curves? *Math. Ann.* **214** (1975), 35–47.
- [9] F. Oort, Endomorphism algebras of abelian varieties. *Algebraic geometry and commutative algebra, in honor of M. Nagata* (1988), 469–502.
- [10] G. Prasad and A. Rapinchuk, Computation of the metaplectic kernel. *Inst. Hautes Études Sci. Publ. Math.* **84** (1996), 91–187.
- [11] I. Reiner, *Maximal orders*. London Mathematical Society Monographs, No. **5**. Academic Press, London-New York, 1975, 395 pp.
- [12] Sheng-Chi Shih, Tse-Chung Yang and C.-F. Yu, Embeddings of fields in simple algebras over global fields. arXiv:1108.0830. 27 pp.
- [13] J. Tate, Endomorphisms of abelian varieties over finite fields. *Invent. Math.* **2** (1966), 134–144.
- [14] J. Tate, Classes d'isogenie de variétés abéliennes sur un corps fini (d'après T. Honda). *Sém. Bourbaki Exp.* 352 (1968/69). Lecture Notes in Math., vol. 179, Springer-Verlag, 1971.
- [15] W. C. Waterhouse, Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)* **2** (1969), 521–560.
- [16] C.-F. Yu, The isomorphism classes of abelian varieties of CM-type. *J. Pure Appl. Algebra* **187** (2004) 305–319.
- [17] C.-F. Yu, On the slope stratification of certain Shimura varieties. *Math. Z.* **251** (2005), 859–873.

- [18] C.-F. Yu, Embeddings of fields into simple algebras: generalizations and applications. *J. Algebra* **368** (2012), 1–20.
- [19] C. Xing, On supersingular abelian varieties of dimension two over finite fields. *Finite Fields Appl.* **2** (1996), no. 4, 407–421.

INSTITUTE OF MATHEMATICS, ACADEMIA SINICA AND NCTS (TAIPEI OFFICE), 6TH FLOOR,
ASTRONOMY MATHEMATICS BUILDING, NO. 1, ROOSEVELT RD. SEC. 4, TAIPEI, TAIWAN, 10617
E-mail address: `chiafu@math.sinica.edu.tw`